PCT/KR 00/00640
RO/KR 19. 06. 2000.

#2

kr 00/640
GJU

10/018944

대 한 민 국 특 허 청

KOREAN INDUSTRIAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Industrial Property Office.

출 원 번 호 : 특허출원 1999년 제 22638 호
Application Number

출 원 년 월 일 : 1999년 06월 17일
Date of Application

출 원 인 : 김동균
Applicant(s)

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

2000 년 06 월 19 일

특 허 청
COMMISSIONER

【서류명】 출원서
【권리구분】 특허
【수신처】 특허청장
【제출일자】 1999.06.17
【발명의 명칭】 이진 정보 보호 전송방법
【발명의 영문명칭】 Binary information transmitting method for protecting the information content

【출원인】
【성명】 김동균
【출원인코드】 4-1999-036303-1
【대리인】
【성명】 박해선
【대리인코드】 9-1998-000229-2
【대리인】
【성명】 조영원
【대리인코드】 9-1998-000529-7
【발명자】
【성명】 김동균
【출원인코드】 4-1999-036303-1
【발명자】
【성명의 국문표기】 배재국
【성명의 영문표기】 BAE, Jaegug
【주민등록번호】 611103-1696230
【우편번호】 606-081
【주소】 부산광역시 영도구 동삼1동
【국적】 KR
【취지】 특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대리인 박해선 (인) 대리인 조영원 (인)

【수수료】
【기본출원료】 20 면 29,000 원
【가산출원료】 0 면 0 원

【우선권주장료】	0 건	0 원
【심사청구료】	0 항	0 원
【합계】	29,000 원	
【첨부서류】	1. 요약서·명세서(도면)_1통 2.위임장_1통	

【요약서】

【요약】

본 발명은 전자 전송매체를 통하여 이진정보를 전송하는 방법에 관한 것으로서, 제 1 단계는 준비작업 단계로서 이진 정보 데이터를 연산처리하기 위한 연산처리 키를 구성하는 단계이다. 제 2 단계는 연산처리화 단계로서 연산처리 키를 이용하여 이진 정보를 전송정보로 변환하는 단계이다. 마지막 단계는 역연산 처리 단계로서 전송된 정보로부터 이진 정보 데이터를 축출하는 단계이다. 제 2 단계와 제 3 단계 사이에 전송정보가 송신국에서 수신국으로 전송된다.

본 발명의 특징은 연산화와 역연산화의 속도가 매우 빠르며, 본 발명에 의한 이진 정보 전송의 안전도는 NP-complete 문제에 근거하고 있다.

【색인어】

이진 정보 보호 전송

【명세서】

【발명의 명칭】

이진 정보 보호 전송방법{Binary information transmitting method for pretecting the infomation content}

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<1> 본 발명은 전자 전송매체를 통하여 이진정보를 전송하는 방법에 관한 것으로써, 특히 이진정보 전송시 제 3 자가 용이하게 전송 데이터의 내용을 파악하지 못하게 하는 상태에서 안전하게 이진정보를 전송하는 방법에 관한 것이다.

<2> 컴퓨터의 사용, 특히 컴퓨터간의 데이터 전송에 있어서 심각한 보안상의 문제가 증가하고 있다. 사실 전송로로부터 전송되는 데이터를 도청하기는 비교적 손쉬운 일이며, 이것은 중요한 정보가 제 3 자의 손으로 넘어갈 수 있다는 것을 의미한다. 이와 같은 위험을 방지하기 위해서 정보 전송시 제 3 자가 용이하게 판독하지 못하도록 정보를 가공한 후 전송할 필요가 있다.

<3> 테이타 통신은 통상 2 진형태로 이루어지고, 이제까지 알려진 전송 시스템의 대부분에 있어서 정보의 가공은 비트 레벨에서 이루어지며 여기서 메시지를 구성하는 '0'과 '1'의 비트열이 코드비트열과 함께 결합된다. 결합된 메시지로부터 전송하고자 하는 정보를 다시 축출해 내기 위해서는 또 다른 코드비트열을 결합 메시지와 결합함으로써 원상으로 복구시킬 수 있다.

<4> 일반적으로 일컬어지는 공개키 보호 전송 방식은 전송하고자 하는 정보 데이터에 일정한 연산처리를 가하기 위한 연산처리 키와 연산처리와 반대 기능을 하는 역연산처리 키 한 쌍을 만들어 사용한다. 연산처리 키는 일반적으로 공개키라 하고 일반 사용자들이 접근가능하도록 공개하며, 역연산처리 키는 개인키라 하고 일반 사용자들이 접근하지 못하도록 비밀로 한다. 송신자는 정보 데이터를 수신자의 공개키로 연산처리한 후 수신자에게 보내고 수신자는 자신의 개인키로 역연산처리함으로써 정보 데이터의 기밀성을 확보하면서 안전하게 이진 정보 데이터를 송수신 할 수 있다.

<5> 1976년 Diffie 와 Hellman 이 처음 소개한 이후로 공개키 전송시스템에 대한 수많은 연구가 진행되어 왔으며, NP-Completeness 인 문제의 어려움에 근거하여 보다 안전한 공개키 전송시스템을 고안하려는 노력이 지속되어 왔다. 공개키 전송시스템의 안정성 여부를 결정하는 가장 중요한 요소는 연산처리 키의 수월성과 역연산처리 키의 NP-Completeness 의 문제에 크게 의존한다.

<6> 그러나, $S = (s_1, s_2, \ldots, s_n)$ 의 양의 정수로 구성된 일련의 정수의 집합에서 $s_i > \sum_{j=1}^{i-1} s_j$ 의 관계를 만족하는 수열을 초증가 수열이라고 하는 데, 초증가 수열의 성질을 공개키에 숨긴 형태의 대부분의 공개키 전송시스템은 Brickell, Lagarias 와 Odlyzko, Schnor 등이 개발한 공격법들에 의해 그 안전성에 심각한 타격을 입게 되었다. 즉, 개인키로 보유하고 있는 역연산처리 키를 제 3 자가 용이하게 찾아내어 정보데이터가 쉽게 유출되는 문제가 발생하였다. 그러한 대부분의 공

격법은 격자기저 축소 알고리즘(Lattice Basis Reduction Algorithm)에 근거한 저밀도(Low Density) 공격법에 의존하고 있다. 지금까지 배낭 문제 (Knapsack Problem) 형태의 공개키 전송시스템은 Chor-Rivest에 의한 것을 포함, 매우 적은 수만이 그러한 공격법에 안전한 것으로 알려져 있다.

<7> RSA는 1978년에 만들어진 공개키 암호시스템으로 현재 세계시장에 90% 이상의 점유율을 갖고 있다. NTRU는 1996년에 만들어진 공개키 암호시스템으로 새로운 형식을 갖는 유망한 시스템이다. 가장 널리 쓰이는 공개키 전송시스템인 RSA 전송시스템은 정수의 소인수분해가 어렵다는 수학적 문제를 기본적인 연산처리 방법으로 삼고 있다. 그러나 RSA 전송시스템은 연산처리화와 역연산처리화에 상당한 시간이 소요된다는 단점을 가지고 있다.

<8> 즉, RSA 와 같은 종래의 장치에 있어서, 코드비트를 발생하는데 시간이 오래걸림으로써 정보의 전달이 지연되었다. 이것은 송신기의 정보의 전송비율을 낮추게 하거나 또는 전송비율을 조절하기 위하여 대용량의 버퍼 등을 구비하는 것이 필요하게 되었다. 후자의 경우는 수신국에서 정보를 수신할 준비가 되어 있지 않다는 신호를 발생할 때 정보가 손실되지 않도록 보장해 주는 조치가 수반되어야 한다.

【발명이 이루고자 하는 기술적 과제】

<9> 따라서 본 발명은 상기와 같은 문제를 해결하기 위한 것으로, 이진 정보 데이터를 제 3 자가 용이하게 파악하지 못하도록 하면서 송신자로부터 수신자로 안전하게 이진 정보 데이터를 전송하고자 하는 것이다.

<10> 본 발명의 또 다른 목적은 종래의 연산처리 및 역연산처리 방식에 비하여 전

송하고자 하는 이진 정보를 가공하는 시간을 단축하므로써 전송 효율를 향상시키기 위한 것이다.

【발명의 구성 및 작용】

<11> 본 발명의 상기 목적은, $k_1 \times k_2$ 가 3 이상의 정수이고, n 이 2 이상의 정수인 경우에 있어서,

<12> $k_1 * k_2$ 로 구성된 n 개의 행렬로 구성된 연산처리 키를 형성하는 단계;

<13> 연산처리 키로부터 $k_1 * k_2$ 로 구성된 n 개의 행렬로 구성된 역연산처리 키를 형성하는 단계;

<14> 송신국은 상기 이진정보를 n 개의 다수 개의 비트열 $E=\{e_1,e_2,\ldots,e_n\}$, $e_i \in \{0,1\}$ 로 분할하는 단계;

<15> 송신국은 다수개의 비트열 E 를 각각 연산처리 키를 이용하여 연산처리하는 단계;

<16> 연산처리된 정보를 합체하여 전송 데이터 S 를 형성하는 단계;

<17> 전송 데이터 S 를 수신국에 전달하는 단계; 및

<18> 수신국은 수신된 상기 전송 데이터 S 를 역연산처리 키를 이용하여 이진정보 데이터를 축출하는 단계를 구비하고, 역연산처리 키를 형성하는 단계가 연산처리 키를 형성하는 단계 후 및 이진정보 데이터를 축출하는 단계 전에 구비함으로써 달성될 수 있다.

<19> 연산처리 키를 형성한 후에, 연산처리 키를 형성하는 각 행렬에 랜덤한 수를 더하거나 또는/및 순서 바꾸기 함수를 실행함으로써 역연산처리 키의 NP-Completeness 인 문제의 어려움을 증가시킬 수 있다. 상기의 경우에 있어서, 역연산처리를 하기 전에 일정한 수를 빼거나 또는/및 순서 바꾸기 함수의 역함수를 실행하여 전송하고자 하는 이진

정보 데이터 E 를 정확하게 축출할 수 있다.

<20> 본 발명은 크게 다음의 중요 3 가지 단계로 구성된다.

<21> 제 1 단계는 준비작업 단계로서 이진 정보 데이터를 연산처리하기 위한 연산처리 키를 구성하는 단계이다. 제 2 단계는 연산처리화 단계로서 연산처리 키를 이용하여 이진 정보를 전송정보로 변환하는 단계이다. 마지막 단계는 역연산 처리 단계로서 전송된 정보로부터 이진 정보 데이터를 축출하는 단계이다. 제 2 단계와 제 3 단계 사이에 전송정보가 송신국에서 수신국으로 전송된다.

<22> 이하에서는 각 단계를 수식적으로 상세히 설명하도록 한다.

<23> 1. 준비작업 단계

<24> (1) 양의 정수 k_1, k_2, l_1, l_2, ... , l_u 를 $k_1 \times k_2 \geq 3,\ 2 \leq u \leq k_1 \times k_2 - 1$ 이 되도록 선택하고, $n = \sum_{s=1}^{u} l_s$ 라고 하자.

<25> (2) 각 s $(1 \leq s \leq u)$ 에 대하여 길이가 l_s 인 초증가 수열(Superincreasing Integer Sequence) u 개를 선택하고 이것을 $d_s = (d_{s,1}, d_{s,2}, \ldots, d_{s,l_s}),\ 1 \leq s \leq u$ 라 하자. 초증가 수열이란 $d_{s,j}$ 가 양의 정수이면서 $\sum_{j=1}^{t} d_{s,j} < d_{s,t+1},\ (1 \leq t \leq l_s - 1)$ 인 수열이다.

<26> (3) 행렬의 크기가 $k_1 \times k_2$ 이고 길이가 n 인 초증가 행렬열 (Superincreasing Matrix Sequence) 을 다음과 같이 구성한다. 이 행렬열을 $cc_t = [cc_{t,(i,j)}]$ 라 하고, $1 \leq t \leq n,\ 1 \leq i \leq k_1,\ 1 \leq j \leq k_2$ 이라 하고 각 $cc_{t,(i,j)}$ 는 다음과 같이 구성한다.

<27>

(ㄱ) 만약 (i,j)=(1,1) 인 경우에, $1 \le t \le l_1$ 이면 $cc_{t,(1,1)} = d_{1,t}$ 로 하고, $l_1+1 \le t \le n$ 이면 $cc_{t,(1,1)}$ 는 양의 임의의 정수 (positive random integer) 로 선택하되 $\sum_{t=l_1+1}^{n} cc_{t,(1,1)} < d_{1,1}$ 를 만족하는 범위에서 선택한다.

<28>

(ㄴ) 만약 (i,j) 가 $2 \le (i-1)k_1+j \le u-1$ 인 경우에, $1 \le t \le \sum_{s=1}^{(i-1)k_1+j-1} l_s$ 이면 $cc_{t,(i,j)}$는 양의 임의의 정수로 선택하고, $\sum_{s=1}^{(i-1)k_1+j-1} l_s+1 \le t \le \sum_{s=1}^{(i-1)k_1+j} l_s$ 이면 $cc_{t,(i,j)} = d_{(i-1)k_1+j,\,t-\sum_{s=2}^{(i-1)k_1+j-1} l_s}$ 로 하고, $\sum_{s=1}^{(i-1)k_1+j} l_s+1 \le t \le n$ 이면 $cc_{t,(i,j)}$는 양의 임의의 정수로 선택하되 $t=\sum_{s=1}^{(i-1)k_1+j} l_s+1$ 를 만족하는 범위에서 선택한다 $\sum_{t=\sum_{s=1}^{(i-1)k_1+j} l_s+1}^{n} cc_{t,(i,j)} < d_{(i-1)k_1+j,1}$

.

<29>

(ㄷ) 만약 (i,j)가 (i-1)k1+j = u 인 경우에, $1 \le t \le \sum_{s=1}^{(i-1)k_1+j-1} l_s$ 이면 $cc_{t,(i,j)}$ 는 양의 임의의 정수로 선택하고, $\sum_{s=1}^{(i-1)k_1+j-1} l_s+1 \le t \le \sum_{s=1}^{(i-1)k_1+j} l_s$ 이면 $cc_{t,(i,j)} = d_{(i-1)k_1+j,\,t-\sum_{s=2}^{(i-1)k_1+j-1} l_s}$ 로 한다.

<30>

(ㄹ) 만약 (i,j) 가 $u+1 \le (i-1)k_1+j \le k_1 \times k_2-1$ 인 경우에 $cc_{t,(i,j)}$, $1 \le t \le n$ 는 양의 임의의 정수로 선택한다.

<31>

(ㅁ) 만약 (i,j) 가 $(i-1)k_1+j = k_1 \times k_2$ 인 경우는 $cc_{t(i,j)} = 0$, $1 \le t \le n$ 으로 선택한다.

<32> (4) 정수 M 을 다음과 같이 선택한다 $M > \mathrm{Max}\{d_{(s,1)}+\sum_{j=1}^{l_s} d_{s,j} \mid s=1,2,\ldots,u\}$.

<33> (5) n 개의 임의의 양의 정수 r_1 , r_2 , ... , r_n 을 선택한다.

<34> (6) 행렬 cc_t 의 각 인수에 r_t 를 더한 후 M 에 의한 잉여류를 선택한 행렬을 수학식 1 과 같이 c_t 라 하자.

<35> 【수학식 1】

$$c_{t,(i,j)} \equiv cc_{t,(i,j)} + r_t \pmod{M}$$

<36> (7) 이제 { 1,2, ...,n } 에 대한 순서 바꾸기 함수 (permutation function) π 를 선택하여 $b_t = c_{\pi(t)}$ 로 구성한다. 상기 cc_t의 각 인수에 r_t를 더하는 단계 또는 순서 바꾸기 함수를 적용하는 단계는 역연산처리 키의 NP-Completeness 문제의 어려움을 증가시키기 위한 것으로서 경우에 따라 생략할 수도 있다.

<37> (8) 각각 크기가 $k_1 \times k_1$와 $k_2 \times k_2$이고, 행렬원소를 M 의 잉여류에 의한 계산을 할 때 역행렬이 존재하도록 두 행렬 w_1 와 w_2 를 임의로 선택한다. 이로써 역연산처리 키 또는 개인키 b_1 , b_2 , ... , b_n , w_1 ,w_2 , M, π 이 완성된다.

<38> (9) n 개의 행렬 $a_t, (1 \le t \le n)$를 다음과 같이 만든다. $a_t \equiv w_1 b_t w_2 \pmod{M}$ 으로 하여 a_t 의 각 원소는 0 과 M 사이에 오도록 한다. 그러면 연산처리 키 또는 공개 키 a_1 , a_2 , ... , a_n 이 완성된다.

<39> 2. <u>연산처리화 단계</u>

<40> 일반적으로 전송하고자 하는 이진 정보를 n 의 비트수로 분할한 후 순서적으로 연

산처리화를 행한다. E 가 0 과 1 만으로 된 길이가 n 인 암호화하고 싶은 평문이라고 하자. 즉, $E=(e_1,e_2,\ldots,e_n),\ e_t\in\{0,1\}$ 이라 한다.

<41> E 를 암호화하기 위해 수학식 2 을 계산하며, 상기 식의 계산 결과는 n 비트에 대한 연산처리화 과정이며, 이러한 연산을 전송하고자 하는 이진정보의 적절한 수만큼 행한 후 상기 연산처리화 결과를 합한 것이 송신국으로부터 수신국으로 전송되는 데이터가 된다.

<42> 【수학식 2】

$$s=\sum_{t=1}^{n}e_t a_t$$

<43> 3. 역연산 처리화 단계

<44> s 으로부터 E 를 복원하는 과정으로 다음과 같은 방식을 취한다.

<45> (ㄱ) w_1 , w_2 의 M 을 잉여류로 한 역행렬 w_1^{-1}, w_2^{-1} 를 구하여, 수학식 3 를 계산한다.

<46> 【수학식 3】

$$s_1\equiv w_1^{-1}sw_2^{-1}\pmod{M}$$

<47> , 여기서 $s_1=[s_{1,(i,j)}]$ 이고 $0\le s_{1,(i,j)}<M$ 인 행렬이다. 그러면 $s_1=\sum_{t=1}^{n}e_t b_t$ 이다.

<48> (ㄴ) 우선 $e'_t=e_{\pi^{-1}(t)}$ 이라 하자. 그러면 $e_t=e'_{\pi(t)}$ 이고 $b_t=c_{\pi(t)}$ 이므로 다음과 같이 쓴다. $s_1=\sum_{t=1}^{n}e_t b_t=\sum_{t=1}^{n}e'_{\pi(t)}c_{\pi(t)}=\sum_{t=1}^{n}e'_t c_t$.

<49>

(ㄷ) 적절한 방정식의 구성과 수학적 귀납법을 이용하여 $(e'_1, e'_2, \ldots e'_n)$의 값을 아래와 같은 방법으로 구한다. 첫번째로 $(e'_1, e'_2, \ldots e'_{l_1})$의 값은 $s_{1,(1,1)} - s_{1,(k_1,k_2)} = \sum_{j=1}^{l_1} x_j d_{1,j}$ 의 방정식에서 $(x_1, x_2, \ldots x_{l_1})$ 의 해가 되는데 $(d_{1,1}, d_{1,2}, \ldots, d_{1,l_1})$ 가 초증가 수열이므로 x_j 의 값을 쉽게 구할 수 있다.

<50>

예를 들어, $s_{1,(1,1)} - s_{1,(k_1,k_2)}$를 계산한 값이 '130' 이고, 초증가 수열이 {30,74,147} 이라 하자. 우선 '130' 은 '147' 보다 작으므로 해는 '0' 으로 되고 연산을 행하지 않고, '130' 은 '74' 와 비교하는 단계가 수행된다. 이 경우 130-74 = 56 으로 연산하며 해는 '1' 로 처리된다. 마지막으로 '56' 은 '30' 과 비교할 때 '56' 이 '30' 보다 크므로 해는 '1' 로 셋팅된다. 따라서 구하고자 하는 최종 해는 {1,1,0} 가 된다. 상기의 문제를 해결은 이 분야의 통상의 지식인에게는 일반적으로 널리 알려진 것이다.

<51>

수학적 귀납법적 가정으로 $(e'_1, e'_2, \ldots e'_w)$ 의 값을 구했다고 가정하자. 여기서 $w = l_1 + l_2 + \ldots + l_v$ 이고 $v \in \{1,2,\ldots,u-1\}$이다. $(e'_{w+1}, e'_{w+2}, \ldots e'_{w+l_{v+1}})$ 의 값은 다음

$$s_v = s_1 - \sum_{t=1}^{w} e'_t b'_t$$

과 같은 방법으로 구한다. 로 놓고 $s_{v,([v/k_2]+1,v+1-[v/k_2])} - s_{v,(k_1,k_2)} = \sum_{j=1}^{l_{v+1}} x_{w+j} d_{v+1,j}$ 의 방정식에서 $(x_{w+1}, x_{w+2}, \ldots, x_{w+l_{v+1}})$ 의 값을 구하면 되는데 역시 $(d_{v+1,1}, d_{v+1,2}, \ldots, d_{v+1,l_{v+1}})$ 가 초증가인 성질을 이용하여 쉽게 $(e'_{w+1}, e'_{w+2}, \ldots, e'_{w+l_{v+1}})$ 를 구할 수 있다. 이 귀납적 방법으로 $(e'_1, e'_2, \ldots, e'_n)$ 을 모두 구한다.

<52> (ㄹ) $e_t = e'_{\pi(t)}$ 인 성질을 이용하여 원래 메시지 $E=(e_1,e_2,\ldots,e_n)$을 다음의 식으로 구한다.

<53> $$E=(e_1,e_2,\ldots,e_n)=(e'_{\pi(1)},e'_{\pi(2)},\ldots,e'_{\pi(n)})$$

【발명의 효과】

<54> 본 발명의 이진 정보 보호 전송방법은 주연산이 덧셈이거나 또는 두 수의 비교이므로 이것은 컴퓨터 상에서 실현하는 데 속도가 거의 걸리지 않는 부분으로서 속도가 매우 빠르며 곱셈을 하는 연산이 없으므로 O(n) 에 비례하게 된다. 이것은 표 1 에 나타낸 바와 같이 기존의 암호시스템에 비하여 매우 빠른 속도이다.

<55> 【표 1】

	본 발명	NTRU	RSA
연산화 속도	n	n^2	n^2
역연산화 속도	n	n^2	n^2
연산 키 길이	n^2	n	n
역연산 키 길이	n^2	n	n
메시지 확장정도	1.5 - 1	3 or 4 -1	1-1

<56> 표 1 에 도시한 바와 같이, 본 발명은 기존의 NTRU 또는 RSA 시스템에 비하여 연산화 및 역연산화 속도가 상당히 빠름을 알 수 있다. 연산처리 키 길이 및 역연산처리 키 길이가 길이가 길어지는 문제는 현재 사용중인 시스템의 메모리 성능의 향상으로 인하여 거의 문제가 되지 않는다.

<57> 따라서, 본 발명은 이진 정보를 전송 매체를 통하여 전송할 경우, 제 3 자가 용이

하게 판독할 수 없도록 함과 동시에 전송 속도를 높일 수 있으므로 홈뱅킹, 전자상거래, 인터넷상에서의 정보교환 등에 직접 응용될 수 있는 효과가 있다.

【특허청구범위】

【청구항 1】

전자 전송 매체를 통하여 다수 개의 비트로 구성된 이진정보를 송신국으로부터 수신국으로 안전하게 전송하는 방법에 있어서, $k_1 \times k_2$ 가 3 이상의 정수이고, n 이 2 이상의 정수일 때,

$k_1 * k_2$ 로 구성된 n 개의 행렬로 구성된 연산처리 키를 형성하는 단계;

상기 연산처리 키로부터 $k_1 * k_2$ 로 구성된 n 개의 행렬로 구성된 역연산처리 키를 형성하는 단계;

상기 송신국은 상기 이진정보를 n 개의 다수 개의 비트열 $E=\{e_1,e_2,\ldots,e_n\}$, $e_i \in \{0,1\}$ 로 분할하는 단계;

상기 송신국은 상기 다수개의 비트열 E 를 각각 상기 연산처리 키를 이용하여 연산처리하는 단계;

상기 연산처리된 정보를 합체하여 전송 데이터 S 를 형성하는 단계;

상기 전송 데이터 S 를 수신국에 전달하는 단계; 및

상기 수신국은 수신된 상기 전송 데이터 S 를 상기 역연산처리 키를 이용하여 상기 이진정보 데이터를 축출하는 단계를 구비하고, 상기 역연산처리 키를 형성하는 단계가 연산처리 키를 형성하는 단계 후 및 이진정보 데이터를 축출하는 단계 전에 구비되는 것을 특징으로 하는 이진 정보 데이터 보호 전송방법.

【청구항 2】

제 1 항에 있어서, 상기 연산처리 키를 형성하는 단계가

2 이상이고 $k_1 * k_2 - 1$ 이하인 임의의 정수 u 를 선택하고, u 개의 양의 정수 $l_1, l_2, \ldots, l_u$를 선택하고, $l_1 + l_2 + \ldots + l_u$의 총합으로 되는 정수 n 을 설정한 후,

$1 \le s \le u$ 의 관계를 만족하는 각 s 에 대하여 길이가 l_s 인 초증가 수열 $d_s = (d_{s,1}, d_{s,2}, \ldots, d_{s,l_s})$ 로 표시되는 u 개의 초증가 수열 $d_1, d_2, \ldots, d_u$를 형성하는 단계;

$Max\left\{ d_{(s,1)} + \sum_{j=1}^{l_s} d_{s,j} \mid s = 1,2,\ldots,u \right\}$ 보다 큰 임의의 정수 M 을 선택하는 단계;

각 행렬 원소를 M 의 잉여류로 계산할 때, 역행렬이 존재하는 임의의 $k_1 * k_1$ 로 구성된 행렬 w_1 및 $k_2 * k_2$ 열로 구성된 행렬 w_2 를 형성하는 단계;

(i,j)=(1,1) 인 경우에, $1 \le t \le l_1$ 이면 $cc_{t,(1,1)} = d_{1,t}$ 로 하고, $l_1 + 1 \le t \le n$ 이면 $cc_{t,(1,1)}$는 양의 임의의 정수로 선택하되 $\sum_{t=l_1+1}^{n} cc_{t,(1,1)} < d_{1,1}$ 를 만족하는 범위에서 선택하고,

(i,j)가 $2 \le (i-1)k_1 + j \le u-1$ 인 경우에, $1 \le t \le \sum_{s=1}^{(i-1)k_1+j-1} l_s$ 이면 $cc_{t,(i,j)}$는 양의 임의의 정수로 선택하고, $\sum_{s=1}^{(i-1)k_1+j-1} l_s + 1 \le t \le \sum_{s=1}^{(i-1)k_1+j} l_s$이면 $cc_{t,(i,j)} = d_{(i-1)k_1+j,\, t - \sum_{s=2}^{(i-1)k_1+j-1} l_s}$ 로 하고, $\sum_{s=1}^{(i-1)k_1+j} l_s + 1 \le t \le n$ 이면 $cc_{t,(i,j)}$는 양의 임의의 정수로 선택하되 $\sum_{t=\sum_{s=1}^{(i-1)k_1+j} l_s + 1}^{n} cc_{t,(i,j)} < d_{(i-1)k_1+j,1}$ 를 만족하는 범위에서 선택하고

(i,j) 가 $(i-1)k_1+j-1$ 인 경우에, $1 \le t \le \sum_{s=1}^{(i-1)k_1+j-1} l_s$ 이면 $cc_{t,(i,j)}$는 양의 임의의 정수로 선택하고, $\sum_{s=1}^{(i-1)k_1+j-1} l_s + 1 \le t \le \sum_{s=1}^{(i-1)k_1+j} l_s$ 이면 $cc_{t,(i,j)} = d_{(i-1)k_1+j,\,t-\sum_{s=2}^{(i-1)k_1+j-1} l_s}$ 로 하고,

(i,j) 가 $u+1 \le (i-1)k_1+j \le k_1 \times k_2-1$ 인 경우에 $cc_{t,(i,j)}$, $1 \le t \le n$는 양의 임의의 정수로 선택하고,

(i,j) 가 $(i-1)k_1+j = k_1 \times k_2$ 인 경우는 $cc_{t(i,j)} = 0$, $1 \le t \le n$ 으로 선택하여 k1×k2 로 구성되는 n 개의 행렬 $cc_{t,(i,j)}$ 를 형성하는 단계;

행렬 cc_t 에 식 $c_{t,(i,j)} \equiv cc_{t,(i,j)} \pmod{M}$ 과 같이 M 의 잉여류를 계산하는 단계; 및

식 $a_t = w_1\, cc_{t,(i,j)}\, w_2 \pmod{M}$ 를 만족하는 연산처리 키 a_t 를 형성하는 단계로 구비되고,

상기 전송 데이터 S 를 형성하는 단계가 $s = \sum_{t=1}^{u} e_t a_t$ 로 이루어지는 것을 특징으로 하고, 상기 M 을 선택하는 단계 및 상기 w_1 과 w_2 를 형성하는 단계가 상기 초증가 수열을 형성하는 단계 후이고 상기 연산처리 키를 형성하는 단계 전에 이루어지는 것을 특징으로 하는 이진 정보 데이터 보호 전송방법.

【청구항 3】

제 2 항에 있어서, n 개의 임의의 양의 정수 r_1, r_2,...,r_n 을 선택한 후, $cc_{t,(i,j)}$ 를 형성하는 단계 및 M 의 잉여류를 계산하는 단계 사이에 행렬 cc_t 의 각 인수에 r_t 를 더하는 단계를 더 구비하는 것을 특징으로 하는 이진 정보 데이터 보호 전송 방법.

【청구항 4】

제 2 항 또는 제 3 항 중 어느 한 항에 있어서, cc_t 의 각 인수에 r_t 를 더하는 단계 또는 r_t 를 더하는 단계가 없는 경우에는 $cc_{t,(i,j)}$ 를 형성하는 단계 및 M 의 잉여류를 계산하는 단계 사이에 n 개의 행렬로 구성된 $cc_{t,(i,j)}$ 행렬에 대한 순서 바꾸기 함수를 실행하는 단계를 더 구비하는 것을 특징으로 하는 이진 정보 데이터 전송방법.

【청구항 5】

제 2 항 또는 제 3 항 중 어느 한 항에 있어서, 상기 이진정보 데이터를 축출하는 단계가

w_1, w_2 의 M 을 잉여류로 하여 역행렬 w_1^{-1}, w_2^{-1} 를 형성하는 단계;

상기 역행렬을 이용하여 하기의 식에 따라 제 1 의 축출전 행렬 s_1 를 형성하는 단계;

$$s_1 = \sum_{t=1}^{n} e_t b_t = w_1^{-1} s w_2^{-1}$$

(여기서 e_i 는 '0' 과 '1' 의 함수이고, b_t 는 $k_1 \times k_2$ 의 행렬임)

$S_{1,(1,1)}-S_{1,(k_1,K_2)}$ 로부터 제 1 비교값을 계산하는 단계;

상기 제 1 비교값과 초증가수열 $\{d_{11},d_{12},\cdots,d_{1l_1}\}$ 로부터 $(e_1,e_2,\cdots,e_{l_1})$ 의 제 1 이진정보를 얻는 단계;

v 가 2 의 값을 갖고, $w=\sum_{j=1}^{v} l_j$ 이라 할 때,

$S_{v,([v/k_2]+1,v+1-[v/k_2])}-S_{v,(k_1,k_2)}$ 로부터 제 v 번째 비교값을 계산하는 단계;

상기 제 v 번째 비교값과 초증가 수열 $(d_{v+1,1},d_{v+1,2},\cdots,d_{v+1,l_{v+1}})$ 로부터 $(e_{w+1},e_{w+2},\cdots,e_{w+l_{v+1}})$ 의 제 v 번째 이진정보를 구하는 단계; 및

상기 제 v 번째 비교값을 계산하는 단계와 제 v 번째 이진정보를 구하는 단계가 v 가 3부터 u 값까지 반복하는 단계를 포함하는 것을 특징으로 하는 이진 정보 데이터 보호 전송방법.

【청구항 6】

제 4 항에 있어서, 상기 이진정보 데이터를 축출하는 단계가

w_1, w_2 의 M 을 잉여류로 하여 역행렬 w_1^{-1},w_2^{-1} 를 형성하는 단계;

상기 역행렬을 이용하여 하기의 식에 따라 제 1 의 축출전 행렬 s_1 를 형성하는 단계;

$s_1 = \sum_{t=1}^{n} e_t b_t = w_1^{-1} s w_2^{-1}$ (여기서 e_i 는 '0' 과 '1' 의 함수이고, b_t 는 $k_1 * k_2$ 의 행렬임)

$s_{1,(1,1)} - s_{1,(k_1,K_2)}$ 로부터 제 1 비교값을 계산하는 단계;

상기 제 1 비교값과 초증가수열 $\{d_{11}, d_{12}, \ldots, d_{1l_1}\}$ 로부터 $(e_1, e_2, \ldots, e_{l_1})$ 의 제 1 이진정보를 얻는 단계;

v 가 2 의 값을 갖고, $w = \sum_{j=1}^{v} l_j$ 이라 할 때,

$s_{v,([v/k_2]+1,\, v+1-[v/k_2])} - s_{v,(k_1,k_2)}$ 로부터 제 v 번째 비교값을 계산하는 단계;

상기 제 v 번째 비교값과 초증가 수열 $(d_{v+1,1}, d_{v+1,2}, \ldots, d_{v+1,l_{v+1}})$ 로부터 $(e_{w+1}, e_{w+2}, \ldots, e_{w+l_{v+1}})$ 의 제 v 번째 이진정보를 구하는 단계;

상기 제 v 번째 비교값을 계산하는 단계와 제 v 번째 이진정보를 구하는 단계가 v 가 3부터 u 값까지 반복하는 단계를 포함하는 단계; 및

상기에서 구한 $(e_1, e_2, \ldots, e_{l_u})$ 에 상기 순서 바꾸기 함수의 역함수를 적용하는 단계를 구비하는 것을 특징으로 하는 이진 정보 데이터 보호 전송방법.